BEST PRIVACY PRACTICES FOR PROTECTING PPI

DEPARTMENT OF THE NAVY

FEBRUARY 2006

DEFINITION

- PROTECTED PERSONAL INFORMATION (PPI)
  - INFORMATION ABOUT AN INDIVIDUAL THAT IDENTIFIES, RELATES TO, IS UNIQUE TO, OR DESCRIBES THAT PERSON.
    - HOME ADDRESS, DATE OF BIRTH, SSN, HOME PHONE, CREDIT CARD NUMBER, ETC

BEST PRACTICES

- BUILD A VISIBLE PRIVACY PROGRAM
- BUILD PRIVACY INTO YOUR BUSINESS PRACTICES
- FORM A PA TEAM TO ADDRESS WAYS TO IMPROVE PROCESSES/ADDRESS NEEDS
- PROPERLY MARK DOCUMENTS AT TIME OF ORIGINATION
- PROPERLY MARK DOCUMENTS FOR TRANSMITTAL
- PROPERLY DISPOSE OF DOCUMENTS

MORE BEST PRACTICES

- MONITOR ACCESS TO DOCUMENTS
- REVIEW BUSINESS PRACTICES TO DETERMINE HOW TO PREVENT LOSS OF CONTROL
- IDENTIFY PA SYSTEMS OF RECORDS USED BY ACTIVITY AND ENSURE THOSE WORKING WITH THE RECORDS ARE TRAINED ON THE SYSTEMS NOTICE
- ENSURE PRIVACY ACT STATEMENTS APPEAR ON DOCUMENTS THAT REQUEST A FIRST PARTY TO SUBMIT PPI

MORE BEST PRACTICES

- ATTEND AND CONDUCT TRAINING
- ESTABLISH A PROTOCOL FOR NOTIFYING AFFECTED INDIVIDUALS AND CNO (DNS-36) SHOULD PPI BE LOST
- CONDUCT AN ANNUAL REVIEW OF YOUR PRIVACY PROGRAM
- ADOPT DON CODE OF PA FAIR INFORMATION PRINCIPLES

BUILD A VISIBLE PRIVACY PROGRAM

- THE ACTIVITY NEEDS TO KNOW WHO YOU ARE AND WHY YOU EXIST
- ENSURE THE COMMAND APPOINTS A PA COORDINATOR
- ISSUE AN IMPLEMENTING INSTRUCTION THAT HIGHLIGHTS COMMAND UNIQUE ISSUES

BUILD PRIVACY INTO YOUR BUSINESS

- IT SAVES TIME, EFFORT, AND MONEY IF YOU BUILD PRIVACY INTO YOUR BUSINESS PRACTICE

FORM A PRIVACY TEAM

- A NECESSITY IN LIGHT OF
  - MOVING FROM PAPER TO ELECTRONIC RECORDS
  - MOVING TO A BLENDED WORKFORCE THAT INCLUDES CONTRACTOR PERSONNEL

PA TEAM

- REVIEW AND APPROVE BEST PRACTICES
- REVIEW COMPLAINTS AND NON-COMPLIANCE
- ASSURE PERSONNEL THAT PA IS A TOP PRIORITY

PA TEAM MEMBERS

- PA COORDINATORS
- PA SYSTEMS OF RECORDS MANAGERS
- IT PROFESSIONALS
- LEGAL STAFF
- TRAINING OFFICERS
- ADMINISTRATIVE SUPPORT PERSONNEL
- CONTRACTING OFFICERS
- SECURITY OFFICER
- PROGRAM OFFICERS

PROPERLY MARK DOCUMENTS

- PROPER MARK DOCUMENTS BEFORE THEY ARE DISTRIBUTED, FAXED, EMAILED, ETC

- REASON: NOT EVERYONE IS ATTUNED TO HOW TO HANDLE DOCUMENTS THEY RECEIVE, PROPER MARKING OF DOCUMENTS ALERTS THE RECIPIENT TO ANY REQUIREMENTS THAT ARE ATTACHED TO THE DOCUMENT

EXAMPLES

- FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED ACCESS MAY RESULT IN CIVIL AND CRIMINAL PENALTIES

- PROVIDE GUIDANCE ON HOW TO RESPOND IF INFORMATION IS RECEIVED IN ERROR

- IF NECESSARY, LIMIT RETRANSMISSION AND/OR DUPLICATION

PROPERLY DISPOSE OF DOCUMENTS

- DOCUMENTS MUST BE DISPOSED OF SO THAT THERE IS NO RISK TO COMPROMISE OF PPI

- BIG ISSUE: AVOID IDENTITY THEFT

MONITOR ACCESS TO DOCUMENTS

- ACCESS TO DOCUMENTS SHOULD BE LIMITED TO THOSE WHO HAVE AN OFFICIAL NEED TO KNOW – NOT A WANT TO KNOW

- DOCUMENTS SHOULD NOT BE PLACED IN AREAS AVAILABLE TO ANYONE

REVIEW BUSINESS PRACTICES

- REVIEW HOW INFORMATION IS STORED AND TRANSMITTED
  - USE OF LAPTOPS
  - BLACKBERRYS
  - RECALL ROSTERS
  - SOCIAL ROSTERS
  - ETC

PA SYSTEMS OF RECORDS NOTICES

- IDENTIFY PA SYSTEMS OF RECORDS USED BY THE ACTIVITY AND ENSURE THOSE USING THE SYSTEMS ARE PROPERLY TRAINED AND HAVE A COPY OF THE NOTICE

- THIS HELPS TO FACILITATE CHANGES TO THE SYSTEM IF BUSINESS PRACTICES CHANGE

USE PRIVACY ACT STATEMENTS

- ANYTIME PPI IS DIRECTLY SOLICITED FROM THE INDIVIDUAL, A PRIVACY ACT STATEMENT (PAS) MUST BE USED.
- A PAS CONTAINS:
  - AUTHORITY
  - PURPOSE
  - ROUTINE USES
  - VOLUNTARY/MANDATORY

ATTEND/CONDUCT TRAINING

- BASED ON LEVEL OF ACTIVITY WITH PPI

  - ORIENTATION TRAINING
  - ANNUAL AWARENESS TRAINING UPDATES
  - SPECIALIZED TRAINING
  - LOTS OF TRAINING RESOURCES AVAILABLE AT HTTP://PRIVACY.NAVY.MIL

LOSS OF PPI

- ESTABLISH PROTOCOL FOR REPORTING LOSS
  - 10 DAY NOTIFICATION TO INDIVIDUALS
  - NOTIFY DNS-36

EXAMPLES OF REPORTED LOSSES OF PPI

- LAPTOP COMPUTER CONTAINING PPI LEFT IN CAR THAT WAS VANDALIZED
- PPI DISPOSED OF IN DUMPSTER AND PAPERS FOUND BLOWING IN WIND
- COMPUTER DATABASE ACCESSED BY UNAUTHORIZED PERSONS
- MEMORY STICK LOST TO COMPUTER
- PPI PLACED IN PUBLIC FOLDER ON WEBSITE
- MESSAGE TRAFFIC NOT PROPERLY MARKED

DON CODE OF PRIVACY ACT FAIR INFORMATION PRINCIPLES

- **DON has devised a list of principles to be applied when handling Protected Personal Information (PPI) . This is referred to as the DON Code of Privacy Act Fair Information Practices.**

- **Any DON employee, military member, or contractor who handles the personal information of others must abide by the principles set forth by the Code.**

The DON Code of Fair Information Principles

1. <u>The Principle of Openness</u>: When we collect personal data from y we will inform you of the intended uses of the data, the disclosures will be made, the authorities for the collection, and whether the coll is mandatory or voluntary. We will collect no data subject to the Priv unless a Privacy Act system notice has been published in the Federa Register and posted on the and at http://privacy.navy.mil.

2. <u>The Principle of Individual Participation</u>: Unless DON has claimed exemption from the Privacy Act, we will, upon request, grant you ac your records; provide you a list of disclosures made outside the Dep of Defense; and make corrections to your file, once shown to be in e

3. <u>The Principle of Limited Collection</u>: DON will collect only those pe data elements required to fulfill an official function or mission groun law. Those collections are conducted by lawful and fair means.

The DON Code of Fair Information Principles (cont'd)

4. The Principle of Limited Retention: DON will retain your personal information only as long as necessary to fulfill the purposes for which is collected. Records will be destroyed in accordance with establishe records management principles.

5. The Principle of Data Quality: DON strives to maintain only accu relevant, timely, and complete data about you.

6. The Principle of Limited Internal Use: DON will use your personal only for lawful purposes. Access to your data will be limited to those Department of Defense individuals with an official need for access.

7. The Principle of Disclosure: DON employees and military member zealously guard your personal data to ensure that all disclosures are with your written permission or are made in strict accordance with t Privacy Act.

The DON Code of Fair Information Principles (cont'd)

8. The Principle of Security: Your personal data is protected by app safeguards to ensure security and confidentiality. Electronic syst be periodically reviewed for compliance with the security principl Privacy Act, the Computer Security Act, and related statutes. Elec collections will be accomplished in a safe and secure manner.

9. The Principle of Accountability: DON and our employees, military members, and contractors are subject to civil and criminal penalti certain breaches of Privacy. DON is diligent in sanctioning individ who violate Privacy rules.

10. The Principle of Challenging Compliance: You may challenge DON you believe that DON has failed to comply with these principles, t Privacy Act, or the rules of a system of records notice. Challenges addressed to the person accountable for compliance with this Cod local Navy/Marine Corps Privacy Act manager, CNO (DNS-36), or CMC (ARSF).